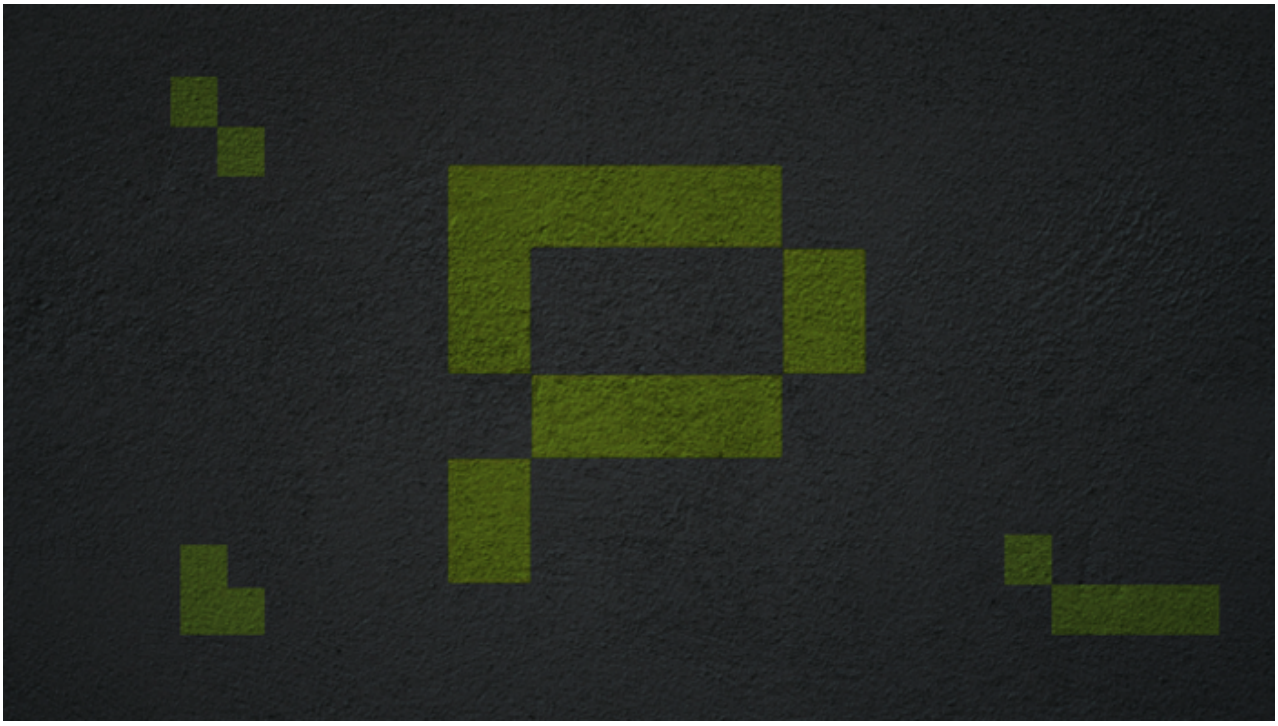
Phala Network : Blockchain-Powered Privacy-Preserving Cloud Computing

leewayhertz.com/what-is-phala



Like any other technology, even blockchain has areas of improvement. It is interesting to see that various new solution-focused blockchain protocols are being developed to overcome the limitations of the technology. For instance, Polkadot resolves the issue of blockchain interoperability. Chainlink enables the communication between on-chain data and off-chain data servers and APIs. Hathor improves scalability and reduces transaction fees.

Likewise, every emerging blockchain protocol is capable of specific strength that further enhances the efficiencies of the blockchain technology, making it more adaptable in the real world.

In this article, we will discuss yet another blockchain protocol called Phala Network. At its core, it is a cloud computing network capable of delivering confidentiality in blockchain smart contracts for dApps and DeFi. Phala seeks to tackle the issue of trust in the computation cloud.

The article will first discuss why smart contract confidentiality is important and how the Phala network facilitates confidentiality. In addition, the article will also cover the other key features of the Phala network and the basic layout of how the network works.

Table of content

Why is confidentiality important in smart contracts?

Blockchain is special because it is a distributed ledger that records transactions in a trustless and transparent way. Every transaction is public. Thus anyone can verify it, yet no one can tamper the data. The transparency of Blockchain is a revolutionary feature that improves security and user sovereignty.

However, businesses also have sensitive and confidential data that they don't want to put on display for everyone to view. For example, stock traders want to make various data public, but they are not fond of revealing their positions or order history. Also, because of lack of confidentiality, even the privacy-related DApps on Ethereum fail to comply with the General Data Protection Regulation. As a result, they may get prevented in European Union.

Not all blockchains are suitable for processing confidential data. Bitcoin and Ethereum are not. Incapability to handle confidential information or business-sensitive data greatly limits the usage of the Blockchain as it creates trust issues.

Several methodologies address the challenge of privacy and confidentiality in Blockchain, but those solutions are limited to cryptocurrencies and don't extend to smart contracts.

What is the Phala Network?

Phala Network is a new approach that seeks to bring confidentiality in smart contracts by utilizing the specialized hardware Trusted Execution Environment (TEE). It aims to provide privacy-preserving smart contracts, to achieve four objectives:

- Protect the privacy of the managed dApps.
- Offer computing power at par with the existing cloud services.
- Maintain the security and trustlessness of Blockchain. All computing operations on Phala are trustless.
- Provide cross-chain interoperability without sacrificing confidentiality.

We discussed in our blockchain interoperability insight, cross-chain communication is necessary for any blockchain dApp or smart contract; otherwise, its application in the real world becomes very limited. Confidential contracts powered by Phala are interoperable, and they can interact with other confidential contracts freely.

Phala blockchain is built on Substrate, so it is naturally interoperable with the Polkadot ecosystem. (Read more about Polkadot interoperability) Also, Phala is a Parachain of Polkadot, so by design itself, it is an interoperable blockchain. However, Phala takes Interoperability a level up by facilitating transferring of assets on another blockchain without compromising on confidentially.

Some key concepts of the Phala Network

Listed below are some of the key concepts that are integral to the Phala network. Knowing them is important to understand how the Phala network adds a layer of confidentiality to smart contracts.

pRunTime stands for Phala Network Secure Enclave Runtime. It is a runtime that executes confidential smart contracts based on confidential computing.

TEE (Trust Execution Environment) is a special hardware component that operates in complete isolation from the rest of the system. It has an independent encrypted memory area, registers, cache, and it operates independently of the operating system, BIOS, virtual machine monitor (VMM) or any other core components.

It is like a BlackBox; what is stored or happening inside TEE is unknown to the outside world. In simple words, TEEs are tamper-proof processors. The Phala network is a network of TEE nodes connected worldwide in a permissionless way.

TEE workers are like Bitcoin or Ethereum Miners. They operate the TEE nodes. Anyone with TEE-supported devices can participate in the Phala network to operate as a worker, but there is a registration process before it. Also, there are Gatekeepers to verify the hardware of the workers and ensure that they are running unmodified pRunTime. Workers are off-chain.

Gatekeepers are like TEE workers. Even they operate on TEE. They also need to get verified and registered with the Phala network. The Gatekeeper serves as the Master key and Contracts key managers. Gatekeepers are also off-chain.

Users are the clients who operate on normal devices. Users don't require TEE to use confidential contracts. They can query and deploy smart contracts and even verify the events on the Blockchain.

Phala Blockchain is the core of the Phala network. It stores identities for all the off-chain communication that happens between the workers, users and gatekeepers. Be it the published confidential contracts, the Worker Nodes, the encrypted contract state, users' invocation transactions, worker state, gatekeeper state, everything is in the Phala blockchain. Also, it can interoperate with other blockchains using the Polkadot relay chain.

How Phala Network confidential smart contract is deployed?

Understand Phala network as two networks: one is the Phala blockchain, and the other is the off-chain TEE network comprising the workers, gatekeepers, and users. The key aspect that imparts confidentiality into Phala smart contracts is the end-to-end encryption of the communication between all the entities, i.e., workers, users and gatekeepers. The TEE is responsible for all the encryption. As mentioned earlier, it is a completely independent tamper-proof processor, so no one can decrypt the information without valid permission. Even workers and gatekeepers themselves cannot take a peek at the contract states. Now let's see how a confidential smart contract is deployed on Phala.

- The client uploads the confidential Contract on the Blockchain.
- The Gatekeep notices the publishing of the Contract and generates a Contract Key for the newly deployed Contract

- The Gatekeeper has the contract key inside his pRuntime, and he also saves it to the Blockchain as a part of the chain state encrypted with Root Key.
- The client can select an available worker for uploading the Contract, and accordingly, the Gatekeeper assigns the contract assignment to a qualified worker after verifying his hardware and pRuntime information. A Contract state map gets stored on the Phala chain
- Once the worker is deployed for the contract assignment, the client sends commands to the Contract on the Blockchain and encrypts the invocation data with a secret generated by the client's private key and the Contract's public key.
- Then, the client also sends a contract query to the worker through off-chain communication. Every communication, on-chain or off-chain, is encrypted and key-protected.
- The worker sets a secured connection with Gatekeeper through his pRuntime and asks for the Contract Key corresponding to the published smart Contract. He uses the Contract Key to recover the keys necessary for Contract state decryption. The pRuntime totally manages the usage of Contract Key for decryption.
- The worker restores the contract state from the Blockchain, decrypts and executes the Contract. CQRS style architecture is used for contract execution.
- Then the worker needs to write back the state updates on the Blockchain. It is mandatory to sign the contract state updates with the Contract key, so the worker can never upload false contract state.
- Then, the worker's pRuntime uses the Contract Key to encrypt the contract state and automatically updates it to the Blockchain in a periodical manner.

What are the key advantages of Phala Network?

- Phala is secured against system-level attacks because sensitive data is processed by TEE, an isolated processor,
- Only key-protected authorized actions are allowed on the network
- All the off-chain and on-chain communication are end-to-end encrypted.
- The off-chain code and execution are verifiable on-chain.
- As a Substrate-based parachain of Polkadot, Phala is designed for Interoperability and cross-chain communication.
- Being interoperable, Phala can offer computing power to other blockchain applications.

What kind of Phala Network development services can LeewayHertz offer?

Phala is all about the privacy and confidentiality of data in cloud computing. As a blockchain development company with the experience of building over 100 digital platforms for startups and enterprises, we are excited to create a completely new range of privacy applications using the Phala network. Privacy-preserving Phala Smart Contracts and dApps are "blockchain+security" products that redefine security concepts in cloud computing.

Development of confidential smart contract

We witness how businesses are increasingly inclined to use smart contracts to improve transparency and security in cross-organizational business transactions. However, the confidentiality of data has always been a point of concern, and some businesses refrain from using smart contracts because they demand a level of privacy in their data.

We seek to help such businesses with confidential smart contract development. Phala smart contracts will not just tackle the issue of data privacy and confidentiality, but these contracts are also interoperable with other confidential smart contracts built on parachains of Polkadot.

IPFS privacy cloud drive development

Cloud storage drives are always subjected to the risk of data leaks, and a major point of concern is that once data are leaked and made public on the Internet, it can never be deleted. IPFS as the decentralized cloud storage solution is much more efficient than centralized cloud storage.

We can combine IPFS and Phala to create a ”privacy cloud storage,” where users can upload data to IPFS with the access rights reserved only to themselves.

Development of privacy applications

We can design a range of privacy blockchain applications for you. We would love to discuss your privacy requirement and brainstorm blockchain dApps to best suit your needs accordingly. Powered by Phala confidential smart contracts, the privacy applications can provide tamper-proof security to your confidential data.

EndNote

Suppose you are looking for smart contracts and blockchain applications for your business but have trust issues because of blockchain transparency. In that case, Phala confidential smart contract is the solution you need. It gives you the security and trustlessness of Blockchain while maintaining the confidentiality of your data. In addition, it also gives you the advantage of Interoperability. To explore the scope of confidential smart contracts for your business, connect with our blockchain experts.